From:	Alperin-Sheriff, Jacob (Fed)
To:	Moody, Dustin (Fed); Liu, Yi-Kai (Fed); Perlner, Ray A. (Fed); internal-pqc
Subject:	Re: Completeness checklists completed
Date:	Thursday, October 19, 2017 12:41:29 PM

I think this covers everything.

From: "Moody, Dustin (Fed)" <dustin.moody@nist.gov>
Date: Thursday, October 19, 2017 at 11:44 AM
To: "Liu, Yi-Kai (Fed)" <yi-kai.liu@nist.gov>, "Perlner, Ray (Fed)" <ray.perlner@nist.gov>, "Alperin-Sheriff, Jacob (Fed)" <jacob.alperin-sheriff@nist.gov>, internal-pqc <internal-pqc@nist.gov>
Subject: Re: Completeness checklists completed

Everyone,
I've updated the draft responses to the submission teams in accordance with your comments. Please let me know if you have any others. The document is attached, and available on the sharepoint site as well.

I've also written up a draft response for what we can post on the forum (and maybe on the FAQ?) as general advice to submitters. It is below, as well as attached. Let me know any comments or suggestions. Thanks,

Dustin

NIST has completed the reviews for all the submissions received by the preliminary deadline, and has sent back comments to each submission team. We note the reviews were to check if submissions were "complete and proper", meeting both our submission requirements and minimal acceptance criteria. They were NOT a review on the technical merits. Submissions which had elements missing will need to revise their submissions, and re-submit by the final deadline of November 30, 2017.

After going through this process, we have some suggestions we think will help submitters to make their submissions complete and proper, as well as help NIST with a more efficient review process following the final deadline.

- Clearly provide ALL of the information on the cover sheet which is asked for in our Call for Proposals (CFP) section 2.A.
- Please clearly and explicitly state which of our five security strength categories your proposed parameter sets meet. See CFP 2.B.4 and 4.A.5.
- Some submissions can be submitted as either a KEM or a public-key encryption scheme, or both. Please clearly indicate which functionality (or functionalities) you want NIST to consider, and include the appropriate required algorithms. See CFP 2.B.1.

- We are interested in qualitative statements about the possible tradeoffs between security and efficiency. That is, besides stating which of the five security strength categories are met, we would like submitters to describe what kind of flexibility there is when adjusting the parameters in their cryptosystem. See CFP 2.B.1.

With regards to the implementations and KATs:

- Please make sure your implementation is platform-independent. See NIST FAQ #3, at https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/faqs
- Please follow our guidance on following the NIST API and generating KATs as posted on our webpage: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Post-Quantum-Cryptography-Standardization/Example-Files
- In addition to the requirement that the README file "shall be a plain text file and list all files that are included on the disc with a brief description of each", it would be useful if the file also contains some basic information about what is being provided. This includes things like how to compile the code, what is produced by the Makefile, and any information necessary to run the files created by the Makefile. On the subject of Makefiles, it would be very useful to have the genKAT and rng files included in the submissions as a concrete example of how to compile the algorithm source code. This will also help facilitate checking of the packages for completeness.

Thank you, and let us know if you have any questions. Specific questions on a submission should be sent to us at pqc-comments@nist.gov. General questions may be posted on the forum, or sent to us the email address just given.

From: Liu, Yi-Kai (Fed)
Sent: Wednesday, October 18, 2017 6:15:47 PM
To: Perlner, Ray (Fed); Alperin-Sheriff, Jacob (Fed); Moody, Dustin (Fed); internal-pqc
Subject: Re: Completeness checklists completed

One minor issue is that several teams submitted both a public key encryption scheme and a KEM, but in some cases it wasn't clear whether they wanted us to evaluate both of those functionalities, or just the KEM. Maybe we should ask submitters to indicate more clearly on this?

Also, we might want to remind the submitters that we're also interested in *qualitative* statements about the possible tradeoffs between security and efficiency. That is, in addition to hitting those security goals (levels 1-5), we're also interested in what kind of flexibility they have when they adjust the parameters in their cryptosystem.

Cheers,

--Yi-Kai

From: Perlner, Ray (Fed)
Sent: Wednesday, October 18, 2017 4:20:37 PM
To: Alperin-Sheriff, Jacob (Fed); Moody, Dustin (Fed); internal-pqc
Subject: RE: Completeness checklists completed

There were a couple of things I recall finding somewhat suspect about pqRSA's security analysis. – in particular the decision to completely ignore quantum attacks with a depth even slightly greater than 2^64, and the assumption that multiplication circuits must be implemented in a fully two dimensional arrangement, despite the fact that modern supercomputers, for example, have significant 3-dimensional connectivity, and therefore look like they could compute a multiplication circuit with about 30 times less latency than he assumes.

From: Alperin-Sheriff, Jacob (Fed)
Sent: Wednesday, October 18, 2017 4:04 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>; internal-pqc <internal-pqc@nist.gov>
Subject: Re: Completeness checklists completed

I edited the part that you wanted me to fix up.

Also, ThreeBears is apparently missing …

From: "Moody, Dustin (Fed)" <dustin.moody@nist.gov<mailto:dustin.moody@nist.gov>>
Date: Wednesday, October 18, 2017 at 3:28 PM
To: internal-pqc <internal-pqc@nist.gov<mailto:internal-pqc@nist.gov>>
Subject: Completeness checklists completed

Everyone,
We have completed all the completeness checklists for the submissions for which we needed to provide feedback for. I have compiled all the information, and written a long word document which includes sample emails to each submission team with what they are missing. It is posted on the sharepoint site, under the main Documents section (and also attached to this email). Please take a look and let me know if you find anything missing, or if I need to change something. I will still add information for each team regarding what signatures we've received to date, but don't worry about that.

We will need to send responses back to each team by the end of the month. I would also like at that time to post a message on the forum with some suggestions for those who will submit before our final deadline. Please let me know if you have any suggestions you think should be passed on. For example, here's a few I've been thinking about:

* Provide all the information on the cover sheet which is asked
* Provide a useful readme file (Larry will give some advice here)
* Please clearly state which of our five security strength categories your parameter sets meet
* Please follow our guidance on following our API and generating KATs as posted on our webpage
* Please make sure your implementation is platform-independent.

The more advice we give to submitters to make our lives easier checking completeness, the better. Thanks everyone!

Dustin